

In the Claims:

Please amend claims 1-4, 6-11, 13-18 and 20-21, add new claims 22-30, and cancel claims 5, 12 and 19, as set forth below.

This listing of claims will replace all prior versions and listings of claims in the application:

1 1. (currently amended) A method for producing ephemeral, symmetric encryption keys at a first
2 station for mutual authentication and secure distribution of a random session-specific symmetric
3 encryption key in a communication session with a second station, comprising:

4 assigning ~~an ephemeral~~ a session key in said the first station, in response to a request to
5 initiate a communication session received by said the first station during a session ~~random~~ key
6 initiation interval for use in a first exchange of said a plurality of exchanges executed for
7 distributing the symmetric encryption key produced for use in the communication session;

8 associating, in said the first station, a set of ephemeral intermediate data ~~random~~ keys,
9 different from said session key, with said request for use in said plurality of exchanges;

10 in the first exchange, sending at least one message carrying said session key to the second
11 station, and receiving a response from the second station including a shared parameter, which is
12 shared between the first station and the second station, or between the first station and a user at
13 the second station, the shared parameter being encrypted using said session random key to verify
14 verifying receipt of the session random key by the second station and to identify the second
15 station or the user of the second station; and

16 in another exchange in the plurality of exchanges, sending, after verifying in said first
17 station receipt of the session ~~random~~ key ~~at~~ by the second station, at least one message carrying
18 an encrypted version of one of the intermediate data keys from said set of ephemeral
19 intermediate data ~~random~~ keys encrypted to be accepted as an the symmetric encryption key for
20 use by the first and second stations during the communication session.

1 2. (currently amended) The method of claim 1, including distributing symmetric encryption keys
2 for use in a plurality of communication sessions using respective pluralities of exchanges, and
3 using assigning said session ~~random~~ key for first exchanges in the respective pluralities of

4 exchanges for initiating communication sessions in the plurality of to all communication
5 sessions initiated with the first station, during said session random key initiation interval, and
6 using other session keys after expiry of said session key initiation interval.

1 3. (currently amended) The method of claim 2 4, including assigning said session random key to
2 all communication sessions initiated with the first station, during said session random key
3 initiation interval, and associating a different associating a unique set of ephemeral intermediate
4 data random keys with each communication session key.

1 4. (currently amended) The method of claim 1, including:
2 providing a buffer at the first station;
3 storing an said ephemeral set of session random keys in the buffer for respective session
4 key lifetimes;

5 associating respective session random key initiation intervals with said ephemeral session
6 random keys stored in said buffer;
7 using session keys from the ephemeral set of session random keys from said buffer as
8 session random keys in response to requests received by said first station during said respective,
9 associated session random key initiation intervals;

10 removing ephemeral session random keys from said buffer upon after expiry of the
11 respective session random key lifetimes lifetime in the buffer.

1 5. (cancel)

1 6. (currently amended) The method of claim 4, wherein a the session random key lifetimes
2 lifetime in the buffer for said plurality of exchanges has a value have respective lengths within
3 which longer or equal to a time required for the plurality of exchanges used to distribute the
4 symmetric encryption key for use in a communication session can be completed in expected
5 circumstances, and said ephemeral session random keys are removed from said buffer after a
6 multiple M times said length value of session random key lifetime to engage into establishing a
7 communication session, where M is less than or equal to 10.

1 7. (currently amended) The method of claim 4, wherein ~~a the session random key lifetimes~~
2 ~~lifetime in the buffer for said plurality of exchanges has a value have respective lengths within~~
3 ~~which which are a multiple M times a time required for the plurality of exchanges used to~~
4 ~~distribute the symmetric encryption key for use in a communication session~~ can be completed in
5 expected circumstances, where M is less than or equal to 10~~and said ephemeral session random~~
6 ~~keys are removed from said buffer after a multiple M times said value, and the session random~~
7 ~~key lifetime to engage into establishing a communication session is less than about 90 seconds.~~

1 8. (currently amended) A data processing apparatus, comprising:

2 a processor associated with a first station, a communication interface adapted for
3 connection to a communication medium, and memory storing instructions for execution by the
4 data processor, the instructions including

5 logic to receive a request via the communication interface for initiation of a
6 communication session between a first station and a second station;

7 logic to provide ephemeral symmetric encryption keys ~~at the first station~~ in response to a
8 request received by said ~~first station~~ processor for initiation of a communication session ~~between~~
9 ~~the first station and the second station, including logic to execute a plurality of exchanges to~~
10 ~~distribute the symmetric encryption key for use in the communication session, logic to provide a~~
11 ~~session key for use~~ during a session ~~random~~ key initiation interval ~~for use in a first exchange of~~
12 ~~said plurality of exchanges, and to associate, in said first station, a set of ephemeral intermediate~~
13 ~~data random keys, different from said session key, with said request for use in said plurality of~~
14 ~~exchanges, and logic to send in a first exchange in said plurality of exchanges~~ at least one
15 message carrying said session ~~random~~ key to the second station, and to receive a response from
16 the second station including a shared parameter encrypted using said session ~~random~~ key
17 ~~verifying to verify receipt of the session random key and to identify the second station or the user~~
18 ~~of the second station; and~~

19 logic to send, after verifying receipt of the session ~~random~~ key at the second station, at
20 least one message carrying, in another exchange in said plurality of exchanges, an encrypted
21 version of one of said set of ~~ephemeral~~-intermediate data ~~random~~ keys ~~encrypted~~ to be accepted
22 as [[an]] the symmetric encryption key for use by the first and second stations during the
23 communication session.

1 9. (currently amended) The apparatus of claim 8, including logic to distribute symmetric
2 encryption keys for use in a plurality of communication sessions using respective pluralities of
3 exchanges, and to use assign said session random key for first exchanges in the respective
4 pluralities of exchanges for distributing the symmetric encryption keys in the plurality of to all
5 communication sessions initiated with the first station, during said session random key initiation
6 interval, and to use other session keys after expiry of said session key initiation interval.

1 10. (currently amended) The apparatus of claim 9, including logic to ~~assign said session~~
2 ~~random key to all communication sessions initiated with the first station during said session~~
3 ~~random key initiation interval, and to associate a different unique set of ephemeral intermediate~~
4 ~~data random keys with each communication session key.~~

1 11. (currently amended) The apparatus of claim 8, including
2 a buffer at the first station;
3 logic to store ~~said ephemeral~~ a set of session random keys in the buffer for respective
4 session key lifetimes, to associate respective session random key initiation intervals with
5 particular session keys in said ephemeral set of session random keys stored in said buffer, to use
6 ephemeral session random keys from said buffer as session random keys in response to requests
7 received by said first station during said respective session random key initiation intervals, and to
8 remove session keys in said ephemeral set of session random keys from said buffer after expiry
9 of the respective session random key lifetimes lifetime in the buffer.

1 12. (cancel)

1 13. (currently amended) The apparatus of claim 11, wherein ~~a the session random key lifetimes~~
2 ~~lifetime in the buffer for said plurality of exchanges has a value have respective lengths within~~
3 ~~which longer or equal to a time required for the plurality of exchanges used to distribute the~~
4 ~~secret encryption key for use in a communication session can be completed in expected~~
5 ~~circumstances, and including logic to remove said session keys in said ephemeral set of session~~
6 ~~random keys from said buffer after a multiple M times said value of expiry of the session random~~
7 ~~key lifetimes lifetime to engage into establishing a communication session, where M is less than~~

8 ~~or equal to 10.~~

1 14. (currently amended) The apparatus of claim 11, wherein ~~a the session random key lifetimes~~
2 ~~lifetime in the buffer for said plurality of exchanges has a value have respective lengths within~~
3 ~~which which are a multiple M times a time required for the plurality of exchanges used to~~
4 ~~distribute the secret encryption key for use in a communication session~~ can be completed in
5 expected circumstances, and including logic to remove said session keys in said ephemeral set of
6 session random keys from said buffer after expiry of a multiple M times said value, and the
7 session random key lifetimes lifetime to engage into establishing a communication session is less
8 than about 90 seconds.

1 15. (currently amended) An article, comprising:

2 machine readable data storage medium having computer program instructions stored
3 therein for establishing a communication session on a communication medium between a first
4 data processing station and a second data processing station having access to the communication
5 medium, said instructions comprising

6 logic to receive a request via the communication interface for initiation of a
7 communication session between a first station and a second station;

8 logic to provide ephemeral symmetric encryption keys ~~at the first station~~ in response to a
9 request received by said ~~first station processor for initiation of a communication session between~~
10 ~~the first station and the second station, including logic to execute a plurality of exchanges to~~
11 ~~distribute the symmetric encryption key for use in the communication session, logic to provide a~~
12 ~~session key for use during a session random key initiation interval for use in a first exchange of~~
13 ~~said plurality of exchanges, and to associate, in said first station, a set of ephemeral intermediate~~
14 ~~data random keys, different from said session key, with said request for use in said plurality of~~
15 ~~exchanges, and logic to send in a first exchange in said plurality of exchanges at least one~~
16 ~~message carrying said session random key to the second station, and to receive a response from~~
17 ~~the second station including a shared parameter encrypted using said session random key~~
18 ~~verifying to verify receipt of the session random key and to identify the second station or the user~~
19 ~~of the second station; and~~

20 logic to send, after verifying receipt of the session ~~random~~ key at the second station, at

21 least one message carrying, in another exchange in said plurality of exchanges, an encrypted
22 version of one of said set of ~~ephemeral~~ intermediate data ~~random~~ keys ~~encrypted~~ to be accepted
23 as [[an]] the symmetric encryption key for use by the first and second stations during the
24 communication session.

1 16. (currently amended) The article of claim 15, wherein the instructions include logic to
2 distribute secret encryption keys for use in a plurality of communication sessions using
3 respective pluralities of exchanges, and to use assign said session ~~random~~ key for first exchanges
4 in the respective pluralities of exchanges for assigning secret encryption keys in the plurality of
5 to all communication sessions initiated with the first station, during said session ~~random~~ key
6 initiation interval, and to use other session keys after expiry of said session key initiation
7 interval.

1 17. (currently amended) The article of claim 16 45, wherein the instructions include logic to
2 ~~assign said session random key to all communication sessions initiated with the first station~~
3 ~~during said session random key initiation interval, and to associate a different unique set of~~
4 ~~ephemeral intermediate data random keys with each communication session key.~~

1 18. (currently amended) The article of claim 15, including
2 a buffer at the first station includes a buffer; and
3 the instructions include logic to store ~~said ephemeral a set of~~ session ~~random~~ keys in the
4 buffer for respective session key lifetimes, to associate respective session ~~random~~ key initiation
5 intervals with particular session keys in said ephemeral set of session ~~random~~ keys stored in said
6 buffer, to use ~~ephemeral~~ session ~~random~~ keys from said buffer as session ~~random~~ keys in
7 response to requests received by said first station during said respective session ~~random~~ key
8 initiation intervals, and to remove session keys in said ephemeral set of session ~~random~~ keys
9 from said buffer after expiry of the respective session ~~random~~ key lifetimes lifetime in the buffer.

1 19. (cancel)

1 20. (currently amended) The article of claim 18, wherein a the session random key lifetimes

2 ~~lifetime in the buffer for said plurality of exchanges has a value have respective lengths within~~
3 ~~which longer or equal to a time required for the plurality of exchanges used to distribute the~~
4 ~~secret encryption key for use in a communication session~~ can be completed in expected
5 circumstances, and the instructions include logic to remove said ~~session keys in said ephemeral~~
6 ~~set of session random~~ keys from said buffer after ~~a multiple M times said value of expiry of the~~
7 ~~session random key lifetimes lifetime to engage into establishing a communication session,~~
8 ~~where M is less than or equal to 10.~~

1 21. (currently amended) The article of claim 18, wherein a ~~the session random key lifetimes~~
2 ~~lifetime in the buffer for said plurality of exchanges has a value have respective lengths within~~
3 ~~which which are a multiple M times a time required for the plurality of exchanges used to~~
4 ~~distribute the secret encryption key for use in a communication session~~ can be completed in
5 expected circumstances, and the instructions include logic to remove said ~~session keys in said~~
6 ~~ephemeral set of session random~~ keys from said buffer after ~~expiry of a multiple M times said~~
7 ~~value, and the session random key lifetimes lifetime to engage into establishing a communication~~
8 ~~session is less than about 90 seconds.~~

1 22. (new) The method of claim 1, wherein the encrypted version of one of said set of
2 intermediate data keys to be accepted as the symmetric encryption key is encrypted using a
3 shared secret credential.

1 23. (new) The method of claim 1, wherein the plurality of exchanges includes an iterative
2 process including n iterations, in which for each iteration (i), the first station sends a message
3 carrying intermediate data key (i) encrypted with intermediate data key (i-1), and the second
4 station obtains intermediate key (i) by decrypting the message with intermediate key (i-1) and
5 returns a message to the first station carrying a hashed version of the intermediate data key (i)
6 encrypted using the intermediate data key (i), until the n-th iteration in which the first station
7 sends intermediate data key (n) as the encrypted version of one of said set of intermediate data
8 keys to be accepted as the symmetric encryption key, encrypted using a first shared secret
9 credential, and the second station, after obtaining intermediate data key (n) by decrypting the
10 message with the first shared secret credential, returns a message to the first station carrying a

11 hashed version of intermediate data key (n) encrypted using the first shared secret credential, and
12 in (n+1)-th iteration, the first station sends intermediate data key (n) encrypted using a second
13 shared secret credential, and the second station, after obtaining intermediate data key (n) by
14 decrypting the message with the second shared secret credential, returns a message to the first
15 station carrying a hashed version of intermediate data key (n) encrypted using the second shared
16 secret credential.

1 24. (new) The method of claim 1, wherein the plurality of exchanges includes an iterative
2 process including n iterations, in which for each iteration (i), the first station sends a message
3 carrying intermediate data key (i) encrypted with intermediate data key (i-1), and the second
4 station obtains intermediate data key (i) by decrypting the message with intermediate data key (i-
5 1), and returns a message to the first station carrying a hashed version of the intermediate data
6 key (i) encrypted using the intermediate data key (i), until the n-th iteration in which the first
7 station sends intermediate data key (n) as the encrypted version of one of said set of intermediate
8 data keys to be accepted as the symmetric encryption key, encrypted using a first shared secret
9 credential and intermediate data key (n-1), and the second station, after obtaining intermediate
10 data key (n) by decrypting the message with the first shared secret credential and intermediate
11 data key (n-1), returns a message to the first station carrying a hashed version of intermediate
12 data key (n) encrypted using the first shared secret credential and intermediate data key (n), and
13 in (n+1)-th iteration the first station sends intermediate data key (n) encrypted using a second
14 shared secret credential and intermediate data key (n), and the second station after obtaining
15 intermediate data key (n) by decrypting the message with the second shared secret credential and
16 intermediate data key (n), returns a message to the first station carrying a hashed version of
17 intermediate data key (n) encrypted using the second shared secret credential and intermediate
18 key (n) .

1 25. (new) The apparatus of claim 8, wherein the encrypted version of one of said set of
2 intermediate data keys to be accepted as the symmetric encryption key is encrypted using a
3 shared secret credential.

1 26. (new) The apparatus of claim 8, wherein the plurality of exchanges includes an iterative

2 process including n iterations, in which for each iteration (i), the first station sends a message
3 carrying intermediate data key (i) encrypted with intermediate data key (i-1), and the second
4 station obtains intermediate key (i) by decrypting the message with intermediate key (i-1) and
5 returns a message to the first station carrying a hashed version of the intermediate data key (i)
6 encrypted using the intermediate data key (i), until the n-th iteration in which the first station
7 sends intermediate data key (n) as the encrypted version of one of said set of intermediate data
8 keys to be accepted as the symmetric encryption key, encrypted using a first shared secret
9 credential, and the second station, after obtaining intermediate data key (n) by decrypting the
10 message with the first shared secret credential, returns a message to the first station carrying a
11 hashed version of intermediate data key (n) encrypted using the first shared secret credential, and
12 in (n+1)-th iteration, the first station sends intermediate data key (n) encrypted using a second
13 shared secret credential, and the second station, after obtaining intermediate data key (n) by
14 decrypting the message with the second shared secret credential, returns a message to the first
15 station carrying a hashed version of intermediate data key (n) encrypted using the second shared
16 secret credential.

1 27. (new) The apparatus of claim 8, wherein the plurality of exchanges includes an iterative
2 process including n iterations, in which for each iteration (i), the first station sends a message
3 carrying intermediate data key (i) encrypted with intermediate data key (i-1), and the second
4 station obtains intermediate data key (i) by decrypting the message with intermediate data key (i-
5 1), and returns a message to the first station carrying a hashed version of the intermediate data
6 key (i) encrypted using the intermediate data key (i), until the n-th iteration in which the first
7 station sends intermediate data key (n) as the encrypted version of one of said set of intermediate
8 data keys to be accepted as the symmetric encryption key, encrypted using a first shared secret
9 credential and intermediate data key (n-1), and the second station, after obtaining intermediate
10 data key (n) by decrypting the message with the first shared secret credential and intermediate
11 data key (n-1), returns a message to the first station carrying a hashed version of intermediate
12 data key (n) encrypted using the first shared secret credential and intermediate data key (n), and
13 in (n+1)-th iteration the first station sends intermediate data key (n) encrypted using a second
14 shared secret credential and intermediate data key (n), and the second station after obtaining
15 intermediate data key (n) by decrypting the message with the second shared secret credential and

16 intermediate data key (n), returns a message to the first station carrying a hashed version of
17 intermediate data key (n) encrypted using the second shared secret credential and intermediate
18 key (n) .

1 28. (new) The article of claim 15, wherein the encrypted version of one of said set of
2 intermediate data keys to be accepted as the symmetric encryption key is encrypted using a
3 shared secret password.

1 29. (new) The article of claim 15, wherein the plurality of exchanges includes an iterative
2 process including n iterations, in which for each iteration (i), the first station sends a message
3 carrying intermediate data key (i) encrypted with intermediate data key (i-1), and the second
4 station obtains intermediate key (i) by decrypting the message with intermediate key (i-1) and
5 returns a message to the first station carrying a hashed version of the intermediate data key (i)
6 encrypted using the intermediate data key (i), until the n-th iteration in which the first station
7 sends intermediate data key (n) as the encrypted version of one of said set of intermediate data
8 keys to be accepted as the symmetric encryption key, encrypted using a first shared secret
9 credential, and the second station, after obtaining intermediate data key (n) by decrypting the
10 message with the first shared secret credential, returns a message to the first station carrying a
11 hashed version of intermediate data key (n) encrypted using the first shared secret credential, and
12 in (n+1)-th iteration, the first station sends intermediate data key (n) encrypted using a second
13 shared secret credential, and the second station, after obtaining intermediate data key (n) by
14 decrypting the message with the second shared secret credential, returns a message to the first
15 station carrying a hashed version of intermediate data key (n) encrypted using the second shared
16 secret credential.

1 30. (new) The article of claim 15, wherein the plurality of exchanges includes an iterative
2 process including n iterations, in which for each iteration (i), the first station sends a message
3 carrying intermediate data key (i) encrypted with intermediate data key (i-1), and the second
4 station obtains intermediate data key (i) by decrypting the message with intermediate data key (i-
5 1), and returns a message to the first station carrying a hashed version of the intermediate data
6 key (i) encrypted using the intermediate data key (i), until the n-th iteration in which the first

7 station sends intermediate data key (n) as the encrypted version of one of said set of intermediate
8 data keys to be accepted as the symmetric encryption key, encrypted using a first shared secret
9 credential and intermediate data key (n-1), and the second station, after obtaining intermediate
10 data key (n) by decrypting the message with the first shared secret credential and intermediate
11 data key (n-1), returns a message to the first station carrying a hashed version of intermediate
12 data key (n) encrypted using the first shared secret credential and intermediate data key (n), and
13 in (n+1)-th iteration the first station sends intermediate data key (n) encrypted using a second
14 shared secret credential and intermediate data key (n), and the second station after obtaining
15 intermediate data key (n) by decrypting the message with the second shared secret credential and
16 intermediate data key (n), returns a message to the first station carrying a hashed version of
17 intermediate data key (n) encrypted using the second shared secret credential and intermediate
18 key (n) .